Temi di Aritmetica Modulare

Incontri Olimpici 2013

SALVATORE DAMANTINO

I.S.I.S. MALIGNANI 2000 - CERVIGNANO DEL FRIULI (UD)

15 Ottobre 2013

1 Relazione di congruenza modulo un intero

Definizione 1.1. Sia n un intero fissato. Si dice che $a, b \in \mathbb{Z}$ sono *congrui* modulo n e si scrive

$$a \equiv b \pmod{n}$$

se $a - b$ è un multiplo di n, cioè esiste $k \in \mathbb{Z}$ tale che $a - b = kn$.

Osservando che se $a - b$ è multiplo di n, è anche multiplo di $-n$, ed escludendo i casi banali in cui $n = 0$ oppure $n = 1$, si può supporre che $n \geq 2$.
Una formulazione equivalente della definizione precedente, ma sicuramente più pratica ed intuitiva, è la seguente:

Proposizione 1.2. *Siano $a, b \in \mathbb{Z}$, $n \geq 2$ intero. Allora $a \equiv b \pmod{n}$ se e solo se a e b hanno lo stesso resto nella divisione per n.*

Dimostrazione. Se $a - b = k \cdot n$, allora $a = kn + b$. Dividendo b per n si ottiene $b = qn + r$, con $0 \leq r < n$ e, sostituendo, $a = (k + q)n + r$, cioè r è anche il resto della divisione di a per n. Viceversa, se $a = q_1 n + r$ e $b = q_2 n + r$, risulta $a - b = (q_1 - q_2)n$, cioè $a \equiv b \pmod{n}$. □

La relazione di congruenza modulo n è una relazione di equivalenza su Z. L'insieme quoziente si indica con $\mathbb{Z}_n$ e si chiama *insieme delle classi di resto modulo n*.
Dalla proposizione precedente segue in particolare che

Corollario 1.3. Ogni intero è congruo modulo n ad uno ed uno soltanto degli interi $0, 1, 2, 3, \ldots, n - 1$.

Tale risultato giustifica la seguente definizione:

Definizione 1.4. Si chiama *sistema completo di residui modulo n* ogni sottoinsieme S di n elementi di $\mathbb{Z}$ tale che ogni $a \in \mathbb{Z}$ è congruo modulo n ad uno ed un solo elemento di S.

Ad esempio $S = \{0,1,2,\dots,n-1\}$ è un sistema completo di residui modulo n, detto *sistema completo minimo modulo n*.
Se n è dispari, allora $S = \left\{-\frac{n-1}{2}, -\frac{n-3}{2}, \dots, -1, 0, 1, \dots, \frac{n-3}{2}, \frac{n-1}{2}\right\}$ è anch'esso un *sistema completo di residui*, detto *minimo in valore assoluto*, modulo n.
Se n è pari, esistono due sistemi completi di residui che hanno la proprietà di minimalità rispetto al valore assoluto e sono:
$S_1 = \left\{-\frac{n-2}{2}, -\frac{n-4}{2}, \dots, -1, 0, 1, \dots, \frac{n-2}{2}, \frac{n}{2}\right\}$ e
$S_2 = \left\{-\frac{n}{2}, -\frac{n-2}{2}, \dots, -1, 0, 1, \dots, \frac{n-4}{2}, \frac{n-2}{2}\right\}$.
Ad esempio, se $n = 7$, il sistema completo minimo di residui è l'insieme $S = \{0,1,2,3,4,5,6\}$; il sistema completo minimo in valore assoluto è l'insieme $S = \{-3,-2,-1,0,1,2,3\}$.
Se $n = 8$, il sistema completo minimo di residui è l'insieme $\{0,1,2,3,4,5,6,7\}$; i sistemi completi minimi in valore assoluto sono gli insiemi $\{-3,-2,-1,0,1,2,3,4\}$ oppure $\{-4,-3,-2,-1,0,1,2,3\}$.
Le congruenze godono di alcune proprietà riassunte nella seguente proposizione:

Proposizione 1.5. *Siano $a,b,c,d \in \mathbb{Z}$, $n \in \mathbb{N}$, $n \geq 2$, e supponiamo che $a \equiv b \pmod{n}$ e $c \equiv d \pmod{n}$. Allora:*

0. $a + k \equiv b + k \pmod{n}$ *per ogni* $k \in \mathbb{Z}$;
1. $a \cdot k \equiv b \cdot k \pmod{n}$ *per ogni* $k \in \mathbb{Z}$;
2. $a + c \equiv b + d \pmod{n}$;
3. $a - c \equiv b - d \pmod{n}$;
4. $a \cdot c \equiv b \cdot d \pmod{n}$;
5. $a^i \equiv b^i \pmod{n}$ *per ogni* $i \in \mathbb{N}$;
6. *se d è un divisore di n allora* $a \equiv b \pmod{d}$.

Altre proprietà sono le seguenti:

Proposizione 1.6. *Se $a \equiv b \pmod{n}$ e $a \equiv b \pmod{m}$, allora $a \equiv b \pmod{z}$, essendo $z = m.c.m.(n,m)$.*

In generale in $\mathbb{Z}_n$ non vale la legge di cancellazione, cioè se $ac \equiv bc \pmod{n}$, in generale non è detto che $a \equiv b \pmod{n}$. Ad esempio

$$15 \equiv 24 \pmod{9}$$

ma non è vero che $5 \equiv 8 \pmod{9}$. Vale tuttavia il seguente risultato.

Proposizione 1.7. *Se $ac \equiv bc \pmod{n}$ e $MCD(c,n) = 1$, allora $a \equiv b \pmod{n}$.*

Si osservi che nell'esempio che abbiamo dato prima non era verificata l'ipotesi richiesta, perchè $\mathrm{MCD}(3,9) = 3 \neq 1$.
Invece, è possibile semplificare per 4 la congruenza $52 \equiv 12 \pmod 5$ in quando $\mathrm{MCD}(4,5) = 1$. Essa quindi diventa $13 \equiv 3 \pmod 5$.

In realtà la proposizione precedente è una conseguenza del seguente risultato più generale.

Proposizione 1.8. *Se* $ac \equiv bc \pmod n$, *allora* $a \equiv b \pmod{\frac{n}{d}}$, *dove* $d = MCD(c,n)$.

Riprendendo l'esempio precedente, $5 \not\equiv 8 \pmod 9$, ma $5 \equiv 8 \pmod{\frac{9}{3}}$.

2 Criteri di divisibilità

Applichiamo la teoria delle congruenze per ritrovare alcuni ben noti criteri di divisibilità, che è possibile generalizzare anche al caso di sistemi di numerazione in base diversa da 10. Ci limitiamo al caso di interi positivi, senza perdita di generalità.

Proposizione 2.1. *Sia* N *un intero positivo tale che ammetta la seguente espressione in base* 10*:*

$$N = a_m 10^m + a_{m-1} 10^{m-1} + a_{m-2} 10^{m-2} + \ldots + a_2 10^2 + a_1 10 + a_0$$

con $0 \leq a_i \leq 9$ *interi,* $0 \leq i \leq m$ *e* $a_m \neq 0$. *Posto*

$$S = \sum_{i=0}^{m} a_i \qquad e \qquad A = \sum_{i=0}^{m} (-1)^i a_i$$

si ha:

(a) N *è divisibile per* 2 *se e solo se* $2 \mid a_0$*;*

(b) N *è divisibile per* 3 *se e solo se* $3 \mid S$*;*

(c) N *è divisibile per* 4 *se e solo se* $4 \mid (a_1 10 + a_0)$*;*

(d) N *è divisibile per* 5 *se e solo se* $5 \mid a_0$*;*

(e) N *è divisibile per* 9 *se e solo se* $9 \mid S$*;*

(f) N *è divisibile per* 11 *se e solo se* $11 \mid A$*;*

(g) sia k *intero tale che* $1 \leq k \leq m$. N *è divisibile per* 2^k *se e solo se* $2^k \mid (a_0 + a_1 10 + \ldots + a_{k-1} 10^{k-1})$.

Dimostrazione. Basta osservare che $10^n \equiv 1 \pmod 3$ e $10^n \equiv 1 \pmod 9$ per ogni $n \in \mathbb{N}$; ancora, $10^n \equiv 0 \pmod{2^k}$ per ogni $n \geq k$ e $10^n \equiv 0 \pmod 5$ per ogni $n \geq 1$; inoltre $10^n \equiv 1 \pmod{11}$ per n pari, $10^n \equiv -1 \pmod{11}$ per n dispari. □

I precedenti criteri di divisibilità in base 10 sono casi particolari di criteri di divisibilità che posso essere formulati in una base b qualunque.
Siano N, b due interi positivi e sia $N = (a_m a_{m-1} \dots a_1 a_0)_b = a_m b^m + a_{m-1} b^{m-1} + \dots + a_1 b + a_0$ la scrittura di N in base b, con $0 \le a_i \le b-1$ interi, $0 \le i \le m$, $a_m \neq 0$.

Proposizione 2.2. *Se d è un intero positivo tale che $d \mid b$ e se $0 < k < m$ allora*

$$d^k \mid N \qquad \Longleftrightarrow \qquad d^k \mid (a_{k-1} a_{k-2} \dots a_0)_b.$$

In particolare, $d \mid N$ se e solo se $d \mid a_0$.

Proposizione 2.3. *Se d è un intero positivo tale che $d \mid b-1$ allora*

$$d \mid N \qquad \Longleftrightarrow \qquad d \mid (a_0 + a_1 + \dots + a_m).$$

Dimostrazione. Basta osservare che

$$d \mid b-1 \qquad \Longleftrightarrow \qquad b \equiv 1 \pmod{d}$$

e dunque

$$N = a_m b^m + \dots + a_1 b + a_0 \equiv a_m + \dots + a_1 + a_0 \pmod{d}.$$

□

Proposizione 2.4. *Se d è un intero positivo tale che $d \mid b+1$ allora*

$$d \mid N \qquad \Longleftrightarrow \qquad d \mid (a_0 - a_1 + a_2 - a_3 + \dots + (-1)^m a_m).$$

Dimostrazione. Basta osservare che

$$d \mid b+1 \qquad \Longleftrightarrow \qquad b \equiv -1 \pmod{d}$$

e dunque

$$N = a_m b^m + \dots + a_1 b + a_0 \equiv (-1)^m a_m + \dots + a_2 - a_1 + a_0 \pmod{d}.$$

□

3 Teorema di Fermat e Teorema di Eulero

Premettiamo la proposizione

Proposizione 3.1. *Per ogni primo p e ogni $x, y \in \mathbb{Z}$ vale la seguente congruenza:*

$$(x+y)^p \equiv x^p + y^p \pmod{p}.$$

Di fondamentale importanza è la seguente proposizione, nota come **Piccolo Teorema di Fermat**.

Proposizione 3.2 (Piccolo Teorema di Fermat)**.** *Sia a un intero e p un numero primo. Allora*

$$a^p \equiv a \pmod{p}.$$

Dimostrazione. Supponiamo $a \geq 0$, per cui possiamo procedere per induzione prendendo come variabile di induzione a stessa. Se $a = 0$ il risultato è ovvio. Supponiamo allora vero il risultato per a, cioè

$$a^p \equiv a \pmod{p},$$

e dimostriamolo per $a+1$. Per la proposizione precedente

$$(a+1)^p \equiv a^p + 1^p.$$

Ma $1^p \equiv 1$ e $a^p \equiv a$ per l'ipotesi induttiva. Quindi

$$(a+1)^p \equiv a+1$$

che è quanto volevamo provare.
Supponiamo ora $a < 0$. Allora $0 \equiv 0^p = (a+(-a))^p \equiv a^p + (-a)^p \pmod{p}$. Dato che è $-a > 0$, per quanto provato al punto precedente è $(-a)^p \equiv -a$, quindi $0 \equiv a^p - a$ cioè $a^p \equiv a \pmod{p}$. □

Ad esempio, risulta $25^{41} \equiv 25 \pmod{41}$, essendo 41 un numero primo.

Una utile applicazione del Piccolo Teorema di Fermat è il suo utilizzo come test di **non primalità** di un numero naturale. Infatti, sappiamo che se p è primo, allora qualunque sia a intero risulta $a^p \equiv a \pmod{p}$. Pertanto possiamo enunciare il seguente test di non primalità.

Proposizione 3.3 (TEST DI NON PRIMALITA')**.** *Se n è un numero naturale tale che esista un $a \in \mathbb{Z}$ verificante la condizione*

$$a^n \not\equiv a \pmod{n},$$

allora n non è primo.

Ad esempio, $n = 6$ è tale che $2^6 \not\equiv 2 \pmod{6}$, quindi 6 non è primo.
Si noti che questo test, pur assicurandoci che il numero non è primo, non ci permette di trovare una fattorizzazione di n. In genere si cerca un a piccolo, in modo da tenere sotto controllo i calcoli, ad esempio si prova con $a = 2$.
Un corollario del Piccolo Teorema di Fermat è la seguente proposizione.

Corollario 3.4. Nelle ipotesi del Piccolo Teorema di Fermat e supposto che $\mathrm{MCD}(a,p) = 1$, risulta

$$a^{p-1} \equiv 1 \pmod{p}.$$

Dimostrazione. Nelle ipotesi attuali possiamo semplificare per a il risultato del Piccolo Teorema di Fermat. □

Analizzando la congruenza $25^{41} \equiv 25 \pmod{41}$, essendo MCD$(25,41) = 1$, possiamo anche scrivere $25^{40} \equiv 1 \pmod{41}$.
Vi sono anche interi k che non sono primi ma per i quali $a^{k-1} \equiv 1 \pmod{k}$ per ogni $a \in \mathbb{Z}$ tale che $MCD(a,k) = 1$. Questi k sono detti numeri di **Carmichael** ed è stato recentemente dimostrato che sono infiniti. I primi numeri di Carmichael sono 561, 1105, 1729. E' possibie generalizzare il risultato contenuto nel Teorema di Fermat riferendosi a moduli arbitrari n e non solamente a moduli primi. Il risultato è del tipo

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Si tratta di scoprire chi è questa funzione $\varphi(n)$, che nel caso in cui n sia un numero primo p deve coincidere con $p-1$.

Definizione 3.5. Sia $n \geq 1$ intero. Si definisce $\varphi(n)$ la funzione di n che rappresenta il numero di interi positivi strettamente minori di n e relativamente primi con n. Essa prende il nome di **funzione di Eulero** o anche **funzione** φ.

Ad esempio, $\varphi(20) = 8$ perchè i numeri minori di 20 e relativamente primi con 20 sono 1, 3, 7, 9, 11, 13, 17, 19.
Le proposizioni che seguono ci permettono di calcolare la funzione di Eulero *per ogni intero n del quale si conosca la fattorizzazione.*

Proposizione 3.6. *Sia $n = p_1^{h_1} p_2^{h_2} \cdots p_s^{h_s}$ la fattorizzazione di n, con i p_i ($i = 1, \ldots, s$) primi distinti. Allora risulta*

$$\varphi(n) = \varphi(p_1^{h_1})\varphi(p_2^{h_2}) \cdots \varphi(p_s^{h_s}).$$

Ad esempio, dato il numero $2016 = 2^5 \cdot 3^2 \cdot 7$, risulta $\varphi(2016) = \varphi(2^5) \cdot \varphi(3^2) \cdot \varphi(7)$. Con il precedente risultato a disposizione siamo ridotti a dover calcolare il valore di φ sulle potenze di un primo, ossia $\varphi(p^h)$.

Proposizione 3.7. *Se p è un numero primo, allora per ogni $h \geq 1$ intero risulta*

$$\varphi(p^h) = p^h - p^{h-1}.$$

Dimostrazione. Basta osservare che non sono primi con p^h solo i multipli di p, e questi sono del tipo:

$$p \cdot i, \qquad 1 \leq i \leq p^{h-1}$$

e quindi sono in numero di p^{h-1}. Quindi il numero di interi positivi minori di p^h e coprimi con p^h è dato da $p^h - p^{h-1}$. □

Osservazione 3.8. Osserviamo che se p è un primo, risulta $\varphi(p) = p-1$. Ad esempio, $\varphi(11) = 11 - 1 = 10$. D'altronde tutti gli interi positivi minori di p (che sono in numero di $p-1$) sono primi con p.

Siamo quindi in grado di calcolare $\varphi(n)$ per ogni $n \in \mathbb{N}$ del quale si conosca la fattorizzazione. Ad esempio, $\varphi(72) = \varphi(2^3 \cdot 3^2) = \varphi(2^3) \cdot \varphi(3^2) = (2^3 - 2^2) \cdot (3^2 - 3) = 4 \cdot 6 = 24$.
Ancora, se $n = 2016$, risulta $\varphi(2016) = \varphi(2^5 \cdot 3^2 \cdot 7) = \varphi(2^5) \cdot \varphi(3^2) \cdot \varphi(7) = (2^5 - 2^4) \cdot (3^2 - 3) \cdot (7 - 1) = 16 \cdot 6 \cdot 6 = 576$.

Di fondamentale importanza è il seguente preannunciato

Proposizione 3.9 (Teorema di Eulero)**.** *Se a ed n sono due interi positivi tali che* $MCD(a, n) = 1$, *allora*

$$a^{\varphi(n)} \equiv 1 \pmod{n}.$$

Ad esempio, se $n = 21$ e $a = 10$, essendo $\mathrm{MCD}(10, 21) = 1$, risulta $10^{\varphi(21)} \equiv 1 \pmod{21}$, cioè, visto che $\varphi(21) = \varphi(3 \cdot 7) = \varphi(3) \cdot \varphi(7) = 2 \cdot 6 = 12$, $10^{12} \equiv 1 \pmod{21}$.

Vediamo come è possibile risolvere problemi di aritmetica modulare applicando il Teorema di Eulero.

Esempio 3.1. Determinare le ultime due cifre della rappresentazione decimale dei numeri 9^{201} e 3^{950}.
Osserviamo che $\varphi(100) = \varphi(5^2 \cdot 2^2) = (5^2 - 5)(2^2 - 2) = 40$ e quindi $9^{\varphi(100)} = 9^{40} \equiv 1 \pmod{100}$. Ne segue che $9^{201} = (9^{40})^5 \cdot 9 \equiv 9 \pmod{100}$ e quindi il resto della divisione di 9^{201} per 100 è pari a 9, cioè le ultime due cifre di 9^{201} sono 09.
D'altra parte, sempre per il Teorema di Eulero, $3^{40} = 3^{\varphi(100)} \equiv 1 \pmod{100}$, quindi $3^{950} = 3^{40 \cdot 23} \cdot 3^{30} = (3^{40})^{23} \cdot (3^5)^6 \equiv 1 \cdot 43^6 \equiv 49^3 \equiv 49 \pmod{100}$. Ne segue che le ultime due cifre del numero 3^{950} sono 49.

Esempio 3.2. Se un intero positivo n è prodotto di due primi distinti, la conoscenza di $\varphi(n)$ equivale a saper fattorizzare n. Infatti, se $n = p \cdot q$, risulta $\varphi(n) = (p - 1)(q - 1)$, e quindi risolvendo il sistema

$$\begin{cases} pq = n \\ (p-1)(q-1) = \varphi(n) \end{cases}$$

è possibile determinare p e q e quindi la fattorizzazione di n.
Ad esempio, se $n = 2279$ e $\varphi(2279) = 2184$, sapendo che $n = p \cdot q$, risolvendo il sistema

$$\begin{cases} pq = 2279 \\ (p-1)(q-1) = 2184 \end{cases}$$

si trova $p = 43$ e $q = 53$, cioè $2279 = 43 \cdot 53$.

Una conseguenza del Teorema di Eulero è il Teorema di Wilson, che rappresenta anche un test di primalità.

Proposizione 3.10 (Teorema di Wilson)**.** *Se p è un numero primo, allora*

$$(p-1)! \equiv -1 \pmod{p}$$

.

Vale anche la seguente generalizzazione.

Proposizione 3.11 (Teorema di Wilson generalizzato)**.** *Un intero positivo n è primo se e solo se* $(n-1)! \equiv -1 \pmod{n}$.

4 Residui quadratici ed equazioni diofantee

Le equazioni diofantee sono equazioni algebriche a coefficienti interi di cui si cercano soluzioni intere. Le congruenze possono essere usate per mostrare che certe equazioni diofantee non hanno soluzione. Mostriamo ad esempio che l'equazione

$$x^2 + y^2 = 39723$$

non ha soluzioni x, y intere. Possiamo ridurre questa equazione modulo 4: a destra troviamo 39723, e

$$39723 \equiv 23 \equiv 3 \pmod{4}.$$

E' possibile che la somma a sinistra sia congrua a 3 modulo 4? Un quadrato è congruo a 0 oppure a 1 modulo 4, quindi $x^2 + y^2$ può essere congruo a 0, a 1 oppure a 2 modulo 4. Ne segue che il primo membro dell'equazione $x^2 + y^2 = 39723$ non può mai essere congruo a 3 modulo 4. Pertanto questa equazione diofantea non ha soluzioni.
Tutti i possibili quadrati modulo 4 si chiamano *residui quadratici modulo 4*. In generale i *residui quadratici modulo d* sono quei resti modulo d che si ottengono dividendo un quadrato per d. Per alcuni valori di d vi sono pochi residui quadratici modulo d: tali valori d costituiscono dei validi test per mostrare che certe equazioni diofantee non hanno soluzione.

Proposizione 4.1. ***Residui quadratici***
Il quadrato di un intero è congruo a 0 oppure a 1 modulo 4, cioè i residui quadratici modulo 4 *sono 0 e 1.*
Il quadrato di un intero è congruo a 0 oppure a 1 modulo 3, cioè i residui quadratici modulo 3 *sono 0 e 1.*
Il quadrato di un intero è congruo a 0, 1 o -1 modulo 5, cioè i residui quadratici modulo 5 *sono 0, 1 e -1.*
Il quadrato di un intero è congruo a 0, 1 o 4 modulo 8, cioè i residui quadratici modulo 8 *sono 0, 1 e 4.*
Il quadrato di un intero è congruo a 0, 1, 4 o 9 modulo 16, cioè i residui quadratici modulo 16 *sono 0, 1, 4 e 9.*

5 Interi esprimibili come somma di due quadrati

Uno dei classici problemi di teoria dei numeri è quello di determinare quali interi sono esprimibili come somma di due quadrati. La parte più ardua della que-

stione è stata, storicamente, quella di esprimere ogni primo della forma $4m+1$ come somma di due quadrati. Il resto è abbastanza semplice.
Innanzitutto osserviamo che, a parte 2 e 3, tutti i numeri primi sono della forma $4m+1$ e $4m+3$. Si può dimostrare che esistono infiniti numeri primi sia del primo tipo che del secondo.
Il fatto che un primo possa esprimersi come somma di due quadrati è strettamente legato al fatto che -1 sia un residuo quadratico modulo tale primo.
Osserviamo innanzitutto che -1 è un residuo quadratico modulo 2. Infatti, la congruenza $x^2 \equiv -1 \pmod 2$ ha soluzione (unica) $x = 1$ modulo 2.

Proposizione 5.1. *Se p è un primo dispari, allora $x^2 \equiv -1 \pmod p$ ha soluzioni se e solo se p è della forma $4m+1$. In tal caso le due soluzioni modulo p sono date da $(\frac{p-1}{2})!$ e $p-(\frac{p-1}{2})!$.*

Dimostrazione. Supponiamo che s sia una soluzione di $x^2 \equiv -1 \pmod p$, cioè $s^2 \equiv -1 \pmod p$. Per il Teorema di Eulero, risulta $s^{p-1} \equiv 1 \pmod p$ e quindi $(s^2)^{\frac{p-1}{2}} \equiv 1 \pmod p$, cioè $(-1)^{\frac{p-1}{2}} \equiv 1 \pmod p$. Da ciò segue che $\dfrac{p-1}{2}$ è pari e quindi $p = 4m+1$.
Viceversa, supponiamo che $p = 4m+1$. Per il Teorema di Wilson, si ha $(p-1)! \equiv -1 \pmod p$. D'altra parte risulta:

$$(p-1)! = 2\cdot 3\cdot 4\cdots(\frac{p-1}{2})\cdot(p-\frac{p-1}{2})\cdots(p-2)\cdot(p-1)$$

da cui, riducendo modulo p,

$$(p-1)! \equiv (-1)^{\frac{p-1}{2}}\cdot\left[\left(\frac{p-1}{2}\right)!\right]^2 \pmod p.$$

Da ciò segue che

$$\left[\left(\frac{p-1}{2}\right)!\right]^2 \equiv -1 \pmod p$$

e cioè $x^2 \equiv -1 \pmod p$ ammette soluzioni. □

Il passo successivo è mostrare che ogni primo p della forma $4m+3$ non è somma di quadrati. Si veda a tal proposito l'esercizio 6.3.
Si dimostra, inoltre, che

Proposizione 5.2. *Ogni primo della forma $p = 4m+1$ è esprimibile come somma di due quadrati, cioè $p = x^2+y^2$ con $x, y \in \mathbb{N}$.*

Infine, si può dimostrare che:

Proposizione 5.3. *Il prodotto della somma di due quadrati è ancora una somma di due quadrati, cioè:*

$$(a^2+b^2)(c^2+d^2) = (ac+bd)^2+(ad-bc)^2.$$

A questo punto siamo in grado di caratterizzare gli interi esprimibili come somma di quadrati:

Proposizione 5.4. *Un intero (naturale) n è esprimibile come somma di due quadrati se e solo se ogni fattore primo della forma $4m+3$ compare con esponente pari nella fattorizzazione di n.*

Dimostrazione. Diremo *rappresentabile* ogni intero n esprimibile come somma di due quadrati.
Supponiamo che $p = 4m+3$ compaia con esponente pari nella fattorizzazione di n. Allora la tesi segue dal fatto che

- 1 e 2 sono rappresentabili;
- il prodotto di due numeri rappresentabili è un numero rappresentabile;
- se n è rappresentabile allora anche nz^2 è rappresentabile. Infatti, se $n = x^2+y^2$, allora $nz^2 = (xz)^2+(yz)^2$.

Supponiamo adesso che n sia rappresentabile e sia $p = 4m+3$ un primo che divide n. Allora, supposto $n = x^2+y^2$, p divide sia x che y. Infatti, se $x \not\equiv 0 \pmod{p}$, allora x avrebbe inverso moltiplicativo k modulo p, cioè $xk \equiv 1 \pmod{p}$. Moltiplicando la $x^2+y^2 \equiv 0 \pmod{p}$ per k^2 si ottiene $(xk)^2+(yk)^2 \equiv 1+(yk)^2 \equiv 0 \pmod{p}$, cioè $(yk)^2 \equiv -1 \pmod{p}$ e ciò è assurdo in quanto -1 non è un residuo quadratico modulo $p = 4m+3$.
Quindi p^2 è un divisore di n. Da cui la tesi. □

Vediamo un esempio.

Esempio 5.1. Il numero 204085 è esprimibile come somma di due quadrati. Infatti $204085 = 5\cdot 7^4\cdot 17$. Si ha $5 = 1^2+2^2$, $17 = 1^2+4^2$, quindi

$$5\cdot 17 = (1^2+2^2)\cdot(1^2+4^2) = (1+8)^2+(4-2)^2 = 9^2+2^2.$$

Quindi $204805 = (7^2\cdot 9)^2+(7^2\cdot 2)^2 = (441)^2+(98)^2$.

6 Problemi

Problema 6.1. Siano dati dieci numeri interi arbitrari, tutti distinti. Provare che sicuramente due di essi differiscono per un multiplo di 9.

Problema 6.2. Si provi che per ogni $n \in \mathbb{N}$ il numero

$$2n^{17}+2n^{15}+3n^3+3n$$

è divisibile per 5.

Problema 6.3. Si dimostri che nessun numero naturale della forma $4n+3$ può scriversi come somma di due quadrati.

Problema 6.4. Trovare tutte le soluzioni naturali dell'equazione $2^m - n^2 = 1$.

Problema 6.5. Dimostrare che se p è un numero primo diverso da 2, 3, 5, allora p divide il numero $u_p = 111\ldots1$ costituito da $p-1$ cifre uguali a 1.

Problema 6.6. Dimostrare che ogni numero naturale ha la stessa cifra finale della sua quinta potenza.

Problema 6.7. Quanti sono i numeri di 5 cifre che non contengono zeri e sono multipli di 12?

Problema 6.8. Sia n un intero positivo e siano $a_1, a_2, \ldots, a_k$ ($k \geq 2$) interi distinti scelti in $\{1, 2, 3, \ldots, n\}$ tali che n divide $a_i(a_{i+1}-1)$ per $i = 1, 2, \ldots, k-1$. Dimostrare che allora n non divide $a_k(a_1 - 1)$.

Problema 6.9. Un intero positivo n è costituito da 500 cifre comprese tra 0 e 7. Letto in base 10 è multiplo di 3, in base 7 è multiplo di 6, in base 16 è multiplo di 15. Quanto può valere al massimo la somma delle cifre di n ?

Problema 6.10. Determinare le soluzioni intere, se esistono, della diofantea $15x^2 - 7y^2 = 9$.

Problema 6.11. Determinare le ultime 8 cifre dell'espansione binaria del numero 27^{1986}.

Problema 6.12. Gli interi $1, 2, 3, \ldots, 1986$ sono scritti in un ordine qualsiasi e concatenati. Dimostrare che non è mai possibile ottenere un cubo perfetto.

Problema 6.13. Dimostrare che in un insieme di n interi, ce ne sono sempre alcuni la cui somma è divisibile per n.

Problema 6.14. Dimostrare che se $2n+1$ e $3n+1$ sono entrambi quadrati perfetti, allora n è divisibile per 40.

Problema 6.15. Sia A la somma delle cifre di 4444^{4444}; sia B la somma delle cifre di A. Quanto vale la somma delle cifre di B?

Problema 6.16. Dimostrare che esistono infiniti numeri primi della forma $6n - 1$.

Problema 6.17. Dimostrare che la diofantea $x^2 + 3xy - 2y^2 = 122$ è impossibile.

7 Soluzioni

Soluzione Problema 6.1. Ricordiamo che $\mathbb{Z}_9$ possiede esattamente 9 elementi, le classi di equivalenza della relazione di congruenza modulo 9, ed ogni intero appartiene ad una e una sola di tali classi. Pertanto, nella migliore delle ipotesi, è possibile scegliere 9 interi a_i distinti, $i = 1, 2, \ldots, 9$, appartenenti ognuno alle 9 classi di equivalenza distinte (uno per classe). Supponiamo che $a_i \in \overline{i-1}$,

$i = 1,2,\dots,9$, cioè a_i appartiene alla classe il cui rappresentante è $i-1$, per $i = 1,\dots,9$. Preso quindi un decimo intero a_{10} distinto dai precedenti, esso apparterrà ad una delle 9 classi di congruenza modulo 9, supponiamo alla classe $\overline{j}$, con $j = i^* - 1$, per qualche $i^* \in \{1,2,\dots,9\}$. Pertanto, essendo anche $a_{i^*} \in \overline{j}$, ne segue che $a_{10} - a_{i^*}$ è un multiplo di 9.

Soluzione Problema 6.2. Se n è un multiplo di 5 il risultato è banalmente vero. Si può allora supporre che $\mathrm{MCD}(n,5) = 1$ e servirsi del Corollario del Piccolo Teorema di Fermat (Corollario 3.4):

$$n^{17} = (n^4)^4 \cdot n \equiv n \pmod 5, \qquad n^{15} = (n^4)^3 \cdot n^3 \equiv n^3 \pmod 5.$$

Quindi

$$2n^{17} + 2n^{15} + 3n^3 + 3n \equiv 2n + 2n^3 + 3n^3 + 3n = 5n + 5n^3 \equiv 0 \pmod 5,$$

cioè $2n^{17} + 2n^{15} + 3n^3 + 3n$ è divisibile per 5 qualunque sia $n \in \mathbb{N}$.

Soluzione Problema 6.3. Supponiamo che esista un numero naturale della forma $4n+3$ che si possa scrivere come somma di due quadrati, cioè $4n+3 = x^2+y^2$, con $x, y \in \mathbb{Z}$. Ma ciò è assurdo perchè $4n+3 \equiv 3 \pmod 4$, mentre x^2+y^2 è congruo a 0, 1 oppure 2 modulo 4 (basta ricordarsi che un quadrato è congruo a 0 oppure 1 modulo 4). Quindi un siffatto numero naturale non può esistere.

Soluzione Problema 6.4. Osserviamo che coppie ordinate (m,n) di soluzioni sono le coppie $(0,0)$ e $(1,1)$. Dimostriamo che non ci sono altre soluzioni oltre alle precedenti. Infatti, osserviamo innanzitutto che le coppie $(1,0)$ e $(0,1)$ non sono soluzioni dell'equazione, come si vede facilmente. Inoltre, se per assurdo $(\overline{m},\overline{n})$ fosse una soluzione dell'equazione $2^m - n^2 = 1$, con $\overline{m},\overline{n} \geq 2$, allora $0 = 2^{\overline{m}} - \overline{n}^2 - 1 \equiv 0 \pmod 4$, ed essendo $2^k \equiv 0 \pmod 4$ qualunque sia $k \geq 2$ intero, si avrebbe $\overline{n}^2 \equiv -1 \equiv 3 \pmod 4$, contro il fatto che nessun quadrato diviso per 4 da resto 3. Quindi le uniche soluzioni sono le coppie $(0,0)$ e $(1,1)$.

Soluzione Problema 6.5. Applichiamo il Corollario al Piccolo Teorema di Fermat rispetto a p e 10 (osserviamo che $\mathrm{MCD}(p,10) = 1$): $10^{p-1} \equiv 1 \pmod p$, per cui p divide $10^{p-1} - 1$. Ma $10^{p-1} - 1 = 9 \cdot u_p$, sicchè p divide $9 \cdot u_p$; ma p non divide 9 (ed è primo), pertanto p divide u_p.

Soluzione Problema 6.6. Dimostrare la tesi equivale a dimostrare che l'ultima cifra del numero $n^5 - n$ è 0, cioè $n^5 - n$ è divisibile per 10.
Ora, se n è divisibile per 10 oppure $n = 0$ oppure $n = 1$, la tesi è banalmente vera. Supponiamo quindi $n \geq 2$ non divisibile per 10.
Se n è divisibile per 2 ma non per 5, si ha $n = 2h$, per qualche h intero non divisibile per 5, da cui

$$n^5 - n = 2h(2h-1)(2h+1)(4h^2+1).$$

Osserviamo ora che uno dei fattori $(2h-1)$, $(2h+1)$ e $(4h^2+1)$ è divisibile per 5. Infatti, se $h \equiv 1 \pmod 5$, risulta $4h^2+1 \equiv 0 \pmod 5$, quindi ad essere divisibile per 5 è il fattore $4h^2+1$; se $h \equiv 2 \pmod 5$, risulta $2h+1 \equiv 0 \pmod 5$, quindi ad essere divisibile per 5 è il fattore $2h+1$; se $h \equiv 3 \pmod 5$, risulta $2h-1 \equiv 0 \pmod 5$, quindi ad essere divisibile per 5 è il fattore $2h-1$; se $h \equiv 4 \pmod 5$, risulta $4h^2+1 \equiv 65 \equiv 0 \pmod 5$, quindi ad essere divisibile per 5 è il fattore $4h^2+1$. Ne segue che $2h(2h+1)(2h-1)(4h^2+1)$ è divisibile per 10, cioè n^5-n è divisibile per 10.
Se n è divisibile per 5 ma non per 2, si ha $n = 5h$, per qualche h intero dispari, da cui

$$n^5 - n = 5h(5^4h^4 - 1)$$

ed osservato che 5^4h^4-1 è pari (perchè differenza di dispari), si ha ancora che n^5-n è divisibile per 10.
Infine, se n non è divisibile nè per 2 nè per 5, allora $\mathrm{MCD}(10,n) = 1$, e quindi, per il Teorema di Eulero, si ha $n^{\varphi(10)} \equiv 1 \pmod{10}$. Ma $\varphi(10) = 4$, quindi $n^4 \equiv 1 \pmod{10}$, da cui $n^5 \equiv n \pmod{10}$, cioè n^5-n è divisibile per 10.

Soluzione Problema 6.7. Imponiamo innanzitutto che il numero sia multiplo di 4. Allora le sue due ultime cifre dovranno essere uno dei multipli di 4 tra 00 e 99; tali multipli sono 25, ma tra questi ve ne sono 7 che contengono almeno uno zero e quindi vanno scartati. Rimaniamo con 18 possibilità per le cifre finali. Ora dobbiamo scegliere altre tre cifre (non zero) di modo che la somma di tutte e cinque le cifre sia multipla di 3, per garantire la divisibilità per 3. Utilizzando le congruenze modulo 3, osserviamo che, per ogni possibile resto della divisione per 3, vi sono esattamente 3 numeri tra 1 e 9 che lo danno (1, 4, 7; 2, 5, 8; 3, 6, 9). A meno dell'ordine, i vari resti modulo 3 si possono ottenere come somma di 3 resti in questi modi: $0 \equiv 0+0+0 \equiv 1+1+1 \equiv 2+2+2 \equiv 0+1+2 \pmod 3$, $1 \equiv 0+0+1 \equiv 1+1+2 \equiv 0+2+2 \pmod 3$, $2 \equiv 0+1+1 \equiv 0+0+2 \equiv 1+2+2 \pmod 3$. Per tenere conto anche dell'ordine, osserviamo che $0+1+2$ si può permutare in 6 modi, $0+0+0$ e simili non hanno permutazioni, tutti gli altri si possono permutare in 3 modi. Quindi, tenendo conto dell'ordine, ogni resto si può scrivere in 9 modi diversi come somma di 3 resti; quindi, fissato un resto, possiamo realizzare un numero di 3 cifre che dia quel resto e che non contenga 0 in $9 \cdot 3^3$ modi e dunque, indipendentemente da quali ultime due cifre scegliamo, avremo $9 \cdot 3^3$ modi di completare il numero di modo che sia multiplo di 3, senza inserire zeri. In totale avremo perciò $18 \cdot 9 \cdot 27 = 4374$ modi.

Soluzione Problema 6.8. Per ipotesi $a_i(a_{i+1}-1) = a_ia_{i+1} - a_i$ è un multiplo di n per $i = 1,\dots,k-1$, cioè $a_i \equiv a_ia_{i+1} \pmod n$ per $i = 1,\dots,k-1$. Esplicitiamo alcune delle precedenti congruenze:

$$\begin{aligned} a_1 &\equiv a_1a_2 \pmod n \\ a_2 &\equiv a_2a_3 \pmod n \\ a_3 &\equiv a_3a_4 \pmod n \end{aligned}$$

$$\vdots$$

Osserviamo adesso che

$$a_1 a_3 \equiv (a_1 a_2) a_3 \equiv a_1 (a_2 a_3) \equiv a_1 a_2 \equiv a_1 \pmod{n},$$

quindi

$$\begin{aligned}
a_1 a_4 \equiv (a_1 a_3) a_4 \equiv a_1 (a_3 a_4) \equiv a_1 a_3 \equiv a_1 \pmod{n} \quad &\Longrightarrow \\
a_1 a_5 \equiv (a_1 a_4) a_5 \equiv a_1 (a_4 a_5) \equiv a_1 a_4 \equiv a_1 \pmod{n} \quad &\Longrightarrow \\
a_1 a_6 \equiv (a_1 a_5) a_6 \equiv a_1 (a_5 a_6) \equiv a_1 a_5 \equiv a_1 \pmod{n} \quad &\Longrightarrow \\
&\vdots \\
a_1 a_k \equiv (a_1 a_{k-1}) a_k \equiv a_1 (a_{k-1} a_k) \equiv a_1 a_{k-1} \equiv a_1 \pmod{n},&
\end{aligned}$$

cioè $a_1 a_r \equiv a_1 \pmod{n}$ per $r = 2, \ldots, k$.
Ora, se per assurdo n dividesse $a_k(a_1 - 1)$, cioè $a_1 a_k - a_k$ fosse multiplo di n o equivalentemente $a_1 a_k \equiv a_k \pmod{n}$, essendo anche $a_1 a_k \equiv a_1 \pmod{n}$, si avrebbe $a_1 \equiv a_k \pmod{n}$, e ciò è in contraddizione col fatto che $a_1, a_k \in \{1, 2, \ldots, n\}$ e sono distinti (quindi la loro differenza non può essere un multiplo di n).
Quindi n non divide $a_k(a_1 - 1)$.

Soluzione Problema 6.9. La somma delle cifre di n è multipla di 3, 6 e 15, quindi di 30. Al massimo può valere $7 \cdot 500 = 3500$. Il più grande multiplo di 30 minore o uguale di 3500 è 3480.

Soluzione Problema 6.10. Riducendo modulo 3 si ottiene $2y^2 \equiv 0 \pmod{3}$, cioè $y = 3h$ per qualche $h \in \mathbb{Z}$. Sostituendo e dividendo per 3 si ottiene $5x^2 - 21h^2 = 3$, da cui $x = 3k$. Sostituendo e dividendo ancora per 3 otteniamo $15x^2 - 7h^2 = 1$, da cui $2h^2 \equiv 1 \pmod{3}$, cioè $h^2 \equiv 2 \pmod{3}$. Assurdo.

Soluzione Problema 6.11. Lavoriamo modulo 256. Si ha $\varphi 256 = 128$ e $1986 = 128 \cdot 15 + 66$. Per il Teorema di Eulero si ha $27^{128} \equiv 1 \pmod{256}$, da cui $27^{1986} \equiv 27^{66} \pmod{256}$. Essendo $27^{64} \equiv 1 \pmod{66}$, si ha che $27^{66} \equiv 27^2 \equiv 217 \pmod{256}$. Scrivendo 217 nel sistema binario si ottiene che le ultime 8 cifre sono 11011001_2.

Soluzione Problema 6.12. Lavorando modulo 9, si ottiene che il numero che si ottiene concatenando casualmente gli interi in questione è congruo alla somma $1 + 2 + \cdots + 1986 = \dfrac{1986 \cdot 1987}{2} = 993 \cdot 1987 \equiv 3 \pmod{9}$. Un cubo non è mai congruo a 3 modulo 9, da cui la tesi.

Soluzione Problema 6.13. Siano a_i, $1 \le i \le n$ gli interi considerati. Poniamo $s_i = a_1 + a_2 + \ldots + a_i$, $i = 1, 2, \ldots, n$. Se uno degli s_i è divisibile per n la tesi è dimostrata, altrimenti ce ne saranno almeno due la cui differenza è divisibile

per n. Siano essi a_h e a_k, con $k > h$. Dato che $a_k - a_h = a_{h+1} + a_{h+2} + \ldots + a_k$, segue la tesi.

Soluzione Problema 6.14. Bisogna dimostrare che n è divisibile sia per 5 che per 8. I quadrati sia modulo 5 che modulo 8 sono $0, 1, -1$, quindi $2n+1 = a$ e $3n+1 = b$ con $a, b \in \{0, 1, -1\}$. Lavoriamo modulo 5. Osserviamo che non può essere $a \neq b$, in quanto, se così fosse, sommando le due relazioni si otterrebbe $2 \equiv a + b \pmod 5$, assurdo. Quindi $a = b$. In tal caso sottraendo le stesse relazioni, si ottiene $n \equiv a - b \equiv 0 \pmod 5$. Di conseguenza n è multiplo di 5.
Analogamente si dimostra la divisibilità per 8. Quindi n è multiplo di 40.

Soluzione Problema 6.15. Essendo $4444 < 10^4$, si ha che $N = 4444^{4444} < (10^4)^{4444} = 10^{17776}$, quindi N possiede meno di 17776 cifre e quindi $A \leq 9 \cdot 17776 = 159984$. Da ciò segue che $B < 54$. Detta C la somma delle cifre di B, risulta $C \leq 13$ (in quanto è 49 il numero di due cifre la cui somma delle cifre è massima). Per trovare C, determiniamo la sua classe di congruenza modulo 9. Si ha, ovviamente, $N \equiv A \equiv B \equiv C \pmod 9$ quindi basta determinare la classe di congruenza di N. Si ha:

$$4444^{4444} \equiv 2^{4444} \equiv (2^6)^{740} \cdot 2^4 \equiv 1 \cdot 16 \equiv 7 \pmod 9.$$

L'unico numero minore o uguale di 13 e congruo a 7 modulo 9 è 7, quindi $C = 7$.

Soluzione Problema 6.16. Osserviamo che se p è un primo maggiore di 3, allora $p \equiv 1, -1 \pmod 6$. Supponiamo che esistono un numero finito di primi della forma $6n - 1$. Consideriamo il numero $N = p! - 1$, essendo p il più grande primo della forma $6n - 1$. Scriviamo N come prodotto di primi:

$$N = p! - 1 = p_1 p_2 \cdots p_m.$$

Osserviamo che ogni p_k è maggiore di p (altrimenti ne esisterebbe uno che divide 1). Poichè p è il più grande congruo a -1 modulo 6, segue che $p_k \equiv 1 \pmod 6$ per ogni k. Da ciò segue che $p! - 1 \equiv 1 \pmod 6$, cioè $p! \equiv 2 \pmod 6$ e ciò è assurdo.

Soluzione Problema 6.17. Risolvendo l'equazione rispetto ad x e riducendo il discriminante modulo 17, si ricava che non può essere un quadrato (lavorare coi residui quadratici modulo 17).